

NIST Special Publication 800-53

Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations Appendix Table D-2

NOTE: THIS DOCUMENT PROVIDES A MARKUP OF CHANGES MADE TO SP 800-53, REVISION 3 APPENDIX TABLE D-2 TO PRODUCE REVISION 4 APPENDIX TABLE D-2. ALTHOUGH A REVIEW WAS MADE TO CONFIRM THE ACCURACY OF THE WORD PROCESSING COMPARISON FUNCTION USED TO IDENTIFY THE CHANGES, THE CHANGES IN SOME CASES WERE CONSIDERABLE, AND THE MARKUP VERSION OF THE CHANGES MAY NOT BE EXACT. AS SUCH, THE MARKUP VERSION SHOULD BE VIEWED AS A GENERAL GUIDE TO THE CHANGES MADE TO REVISION 3 TO PRODUCE REVISION 4 OF SP 800-53. ANY DISCREPANCIES NOTED BETWEEN THE MARKUP AND CLEAN COPIES OF SP 800-53, REVISION 4, PLEASE DEFER TO THE CLEAN COPY FOR THE OFFICIAL VERSION OF

JOINT TASK FORCE TRANSFORMATION INITIATIVE

*Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology*

<http://dx.doi.org/10.6028/NIST.SP.800-53r4>

MARKUP COPY

From: Revision 3 – August 2009
To: Revision 4 – April 2013
INCLUDES UPDATES AS OF 05-07-2013

April 2013

INCLUDES UPDATES AS OF 05-07-2013: PAGE XVII



U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

TABLE D-2: SECURITY CONTROL BASELINES¹

C NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14	AC-14
AC-15	Withdrawn	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P2	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Withdrawn	---	---	---	---

- Deleted: Login
- Moved down [1]: Withdrawn
- Moved (insertion) [2]
- Deleted: ---
- Deleted: ---
- Deleted: ---
- Deleted: ---
- Deleted: (1)
- Deleted: (1)
- Deleted: (5) (7) (8)
- Deleted: (5) (7) (8)
- Deleted: 2 (
- Deleted: 1) (2) (3)
- Deleted: 1) (2) (3)
- Deleted: P0
- Moved up [2]: Not Selected
- Deleted: User-Based Collaboration and
- Deleted: Not Selected
- Moved (insertion) [1]
- Moved down [3]: Contacts with Security Groups and Associations
- Deleted: P0
- Deleted: Not Selected
- Deleted: Not Selected
- Deleted: Not Selected

¹ The security control baselines in Table D-2 are the initial baselines selected by organizations prior to conducting the tailoring activities described in Section 3.2. The control baselines and priority codes are only applicable to non-national security systems. Security control baselines for national security systems are included in CNSS Instruction 1253.

C NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P1	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Withdrawn	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P3	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P3	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P1	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P1	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P2	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11

Deleted: Auditable
 Deleted: (4)
 Deleted: (4)

Deleted: Information
 Deleted: Connections

Deleted: 4
 Deleted: 5) (6)

Deleted: (3)
 Deleted: (3)

Deleted: 1
 Deleted: 1

C NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	Withdrawn	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P1	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P3	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	Not Selected

Deleted: and Exercises
Deleted: (4)

Deleted: (5)
Deleted: (5)

Deleted: (3)
Deleted: 3 (

Deleted: and Exercises
Deleted: 1

C NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected	Not Selected
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	P2	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	P1	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Maintenance Personnel	P1	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P2	Not Selected	MA-6	MA-6
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2	MP-2
MP-3	Media Marking	P2	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected	Not Selected
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P2	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-7	Withdrawn				
PE-8	Visitor Access Records	P3	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P2	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected
Planning					
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2 (3)	PL-2 (3)

- Deleted: (1)
- Deleted: 1 (
- Deleted: Non-Local
- Deleted: 1 (
- Deleted: 1 (
- Deleted: 1
- Deleted: (1)
- Deleted: (1)
- Deleted: 1
- Deleted: 2 (
- Deleted: 2 (3) (
- Deleted: 1
- Deleted: 2
- Deleted: Visitor Control
- Deleted: P1
- Deleted: PE-7
- Deleted: PE-7 (1)
- Deleted: PE-7 (1)
- Deleted: (2)
- Deleted: Power
- Deleted: 1) (2) (
- Deleted: 1
- Deleted: 1
- Deleted: 2
- Deleted: PE-18
- Deleted: (1)

C NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PL-3	Withdrawn	---	---	---	---
PL-4	Rules of Behavior	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	Withdrawn	---	---	---	---
PL-6	Withdrawn	---	---	---	---
PL-7	Security Concept of Operations	P0	Not Selected	Not Selected	Not Selected
PL-8	Information Security Architecture	P1	Not Selected	PL-8	PL-8
PL-9	Central Management	P0	Not Selected	Not Selected	Not Selected
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P1	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	Withdrawn	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected
System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	P1	SA-3	SA-3	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	Information System Documentation	P2	SA-5	SA-5	SA-5
SA-6	Withdrawn	---	---	---	---
SA-7	Withdrawn	---	---	---	---
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected
SA-14	Criticality Analysis	P0	Not Selected	Not Selected	Not Selected
SA-15	Development Process, Standards, and Tools	P2	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	P2	Not Selected	Not Selected	SA-16

- Formatted Table
- Deleted: 1
- Deleted: PL-5
- Deleted: PL-5
- Deleted: PL-5
- Deleted: Not Selected
- Deleted: PL-6
- Deleted: PL-6
- Deleted: Categorization
- Deleted: 2
- Deleted: 3) (
- Deleted: (7)
- Deleted: Support
- Deleted: Acquisitions
- Deleted: 4
- Deleted: 4
- Deleted: (1) (3)
- Deleted: (1) (2) (3)
- Deleted: Software Usage Restrictions
- Deleted: P1
- Deleted: SA-6
- Deleted: SA-6
- Deleted: SA-6
- Deleted: User-Installed Software
- Deleted: P1
- Deleted: SA-7
- Deleted: SA-7
- Deleted: SA-7
- Deleted: 2
- Deleted: P1
- Deleted: SA-13
- Deleted: Critical Information System Components
- Deleted:

C NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-17	Developer Security Architecture and Design	P1	Not Selected	Not Selected	SA-17
SA-18	Tamper Resistance and Detection	P0	Not Selected	Not Selected	Not Selected
SA-19	Component Authenticity	P0	Not Selected	Not Selected	Not Selected
SA-20	Customized Development of Critical Components	P0	Not Selected	Not Selected	Not Selected
SA-21	Developer Screening	P0	Not Selected	Not Selected	Not Selected
SA-22	Unsupported System Components	P0	Not Selected	Not Selected	Not Selected
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Withdrawn	P1	Not Selected	Not Selected	Not Selected
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	Withdrawn	P1	Not Selected	Not Selected	Not Selected
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected

- Deleted: Priority
- Deleted: 1) (2) (
- Deleted: 1) (2) (
- Deleted: 6) (
- Deleted: Transmission Confidentiality
- Deleted: P1
- Deleted: Not Selected
- Deleted: SC-9 (1)
- Deleted: SC-9 (1)
- Deleted: Use of Cryptography
- Deleted: Public Access Protections
- Deleted: P1
- Deleted: SC-14
- Deleted: SC-14
- Deleted: SC-14
- Deleted: SC-14
- Deleted: 1
- Deleted: (1)
- Deleted: (1)
- Deleted: (1)
- Deleted: Not Selected
- Deleted: Not Selected
- Deleted: Not Selected
- Deleted: Operating System
- Deleted: Virtualization Techniques

C NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	Withdrawn	P0	Not Selected	Not Selected	Not Selected
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	Withdrawn	P0	Not Selected	Not Selected	Not Selected
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected
Program Management					
PM-1	Information Security Program Plan	P1	Deployed organization-wide, Supporting information security program. Not associated with security control baselines. Independent of any system impact level.		
PM-2	Senior Information Security Officer	P1			
PM-3	Information Security Resources	P1			
PM-4	Plan of Action and Milestones Process	P1			
PM-5	Information System Inventory	P1			
PM-6	Information Security Measures of Performance	P1			
PM-7	Enterprise Architecture	P1			
PM-8	Critical Infrastructure Plan	P1			
PM-9	Risk Management Strategy	P1			

- Deleted: P1
- Deleted: SC-32
- Deleted: SC-32
- Deleted: Transmission Preparation Integrity
- Deleted: P0
- Deleted: Not Selected
- Deleted: Not Selected
- Deleted: Not Selected

- Deleted: (3)
- Deleted: (3)
- Deleted: Not Selected
- Deleted: (6)
- Deleted: (6)
- Deleted: Functionality
- Deleted: 1
- Deleted: Information Input Restrictions
- Deleted: P2
- Deleted: Not Selected
- Deleted: SI-9
- Deleted: SI-9
- Deleted: Output

- Deleted: all

C					
NTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PM-10	Security Authorization Process	P1	Deployed organization-wide. Supporting information security program. Not associated with security control baselines. Independent of any system impact level.		
PM-11	Mission/Business Process Definition	P1			
PM-12	Insider Threat Program	P1			
PM-13	Information Security Workforce	P1			
PM-14	Testing, Training, and Monitoring	P1			
PM-15	Contacts with Security Groups and Associations	P3			
PM-16	Threat Awareness Program	P1			

Moved (insertion) [3]